AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason M. Guyton, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations (HSI), currently assigned to HSI Cleveland, Ohio. I have been employed with HSI since March 2009. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a) and 2252A(a). I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I teach how to conduct child exploitation investigations to new agents at the HSI Academy and have presented at multiple national conferences related to these investigations. I have written numerous affidavits in support of search and arrest warrants related to investigations of child pornography, online enticement, and other child exploitation crimes. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of search warrants.

2. The statements in this affidavit are based upon my personal knowledge and observations, my training and experience, information obtained from other law enforcement and witnesses, and the review of various documents and records. Because this affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a) are present in the information associated with the accounts **cgalaszewski@gmail.com** and **mckainchris3@gmail.com**. I make this affidavit in support of an application for a search warrant for content and records associated with the above accounts which is stored at a premise owned, maintained, controlled, or operated by Google LLC. ("Google"), an e-mail, remote storage and software provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

3. The information and accounts to be searched is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts referenced in this affidavit and further in Attachment A, including the contents of the communications.

4. I have probable cause to believe that evidence of violations of 18 U.S.C. § 2252A, involving the use of a computer in or affecting interstate commerce to transport, receive, distribute, possess and/or access child pornography is located within the accounts described below. I have reason to believe that the member accounts that are the subject of the instant application will have stored information and communications that are relevant to this investigation, to include evidence of

the identity of the person maintaining the account and other relevant information associated with the user. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the crimes are in these accounts.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, §2252A, and relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, distributing, receiving, reproducing for distribution, possessing or accessing with intent to view any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

6. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled "Stored Wire and Electronic Communications and Transactional Records Access." 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation. 18 U.S.C. § 2510(12) defines "electronic

communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo optical system that affects interstate or foreign commerce," with certain exceptions not applicable here. 18 U.S.C. § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

c. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related

to or operating in conjunction with such device. Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

d. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

e. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings,

painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as flash drives, SD cards, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

f. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static,

if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail account is created by the user.

h. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

i. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

j. A "Preservation Letter" is a letter government entities issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in its possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

k. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

l. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND EMAIL

8. I have both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and

required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access

to a computer and modem.[1] Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

d. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally,

[1] The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

INFORMATION ABOUT GOOGLE, LLC.

9. Based on my training and experience, I know that Google is a company that among other things offers numerous online-based services, including email (Gmail), navigation (Google Maps), online file storage (including Google Drive, Google Photos, and YouTube), messaging (Google Hangouts), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging require the user to sign into the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and YouTube, can be used while signed into a Google account, although some aspects of these services can be use even without being signed into a Google account.

10. Based on my training and experience, I know Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device. The Android OS is the most popular cellphone operating system in the United Sates. As of April 2, 2020, it was the OS on 51.8% of all cellphones in the United States according to www.statista.com.

11. Based on my training and experience, I know that, in the context of mobile computing devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

12. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including tailoring search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising.

13. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and

source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information can often provide clues to their identity, location, or illicit activities.

14. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

15. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user because of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

17. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into

an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications to conceal them from law enforcement).

18. I know from my training and experience that Google preserves the content of the accounts that have been flagged, or at the request of a law enforcement agency preservation request.

INFORMATION ABOUT DROPBOX, INC.

19. Dropbox refers to an online storage medium on the Internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

20. Dropbox is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud,

and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications. Each Dropbox user is afforded 2GB of free storage space that may be used to save photographs, videos, documents, and e-mail messages. Users can manually upload and sync the files on their computer to the Dropbox account or they can set their account to automatically sync files to the Dropbox account after a certain amount of time. The frequency with which someone uploads files to their Dropbox account may be different for each user. For this reason, users may have received and retained files in their regular email account for some time prior to uploading or syncing the files to the Dropbox storage.

21. Dropbox provides a variety of online services, including online storage access, to the public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

INFORMATION REGARDING NCMEC

22. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit organization to serve as a national clearinghouse

and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the Cyber Tipline and Child Victim Identification Programs. NCMEC makes information submitted to the Cyber Tipline and Child Victim Identification Programs available to law enforcement and uses this information to help identify trends and create child safety and prevention messages. As a national clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement, and the public in a combined effort to reduce online child sexual abuse images. NCMEC does not act in the capacity of or under the direction or control of the government or any law enforcement agency. NCMEC does not independently investigate and cannot verify the accuracy of the information submitted by reporting parties.

23. Cyber Tipline Reports are initially submitted to NCMEC. Anyone can submit a Cyber Tipline Report, although the majority of Cyber Tipline Reports I review are submitted by ESPs such as Google, Facebook, Instagram, Yahoo, Microsoft, Dropbox, and the like. Cyber Tipline Reports from ESPs typically contain information about the subscriber, such as the subscriber's username, email address, telephone numbers, and IP address history. Cyber Tipline Reports will also contain the child exploitation material that caused the ESP to initiate the report. That child exploitation material is often image or video files of child pornography as defined by federal law.

STATEMENT OF PROBABLE CAUSE

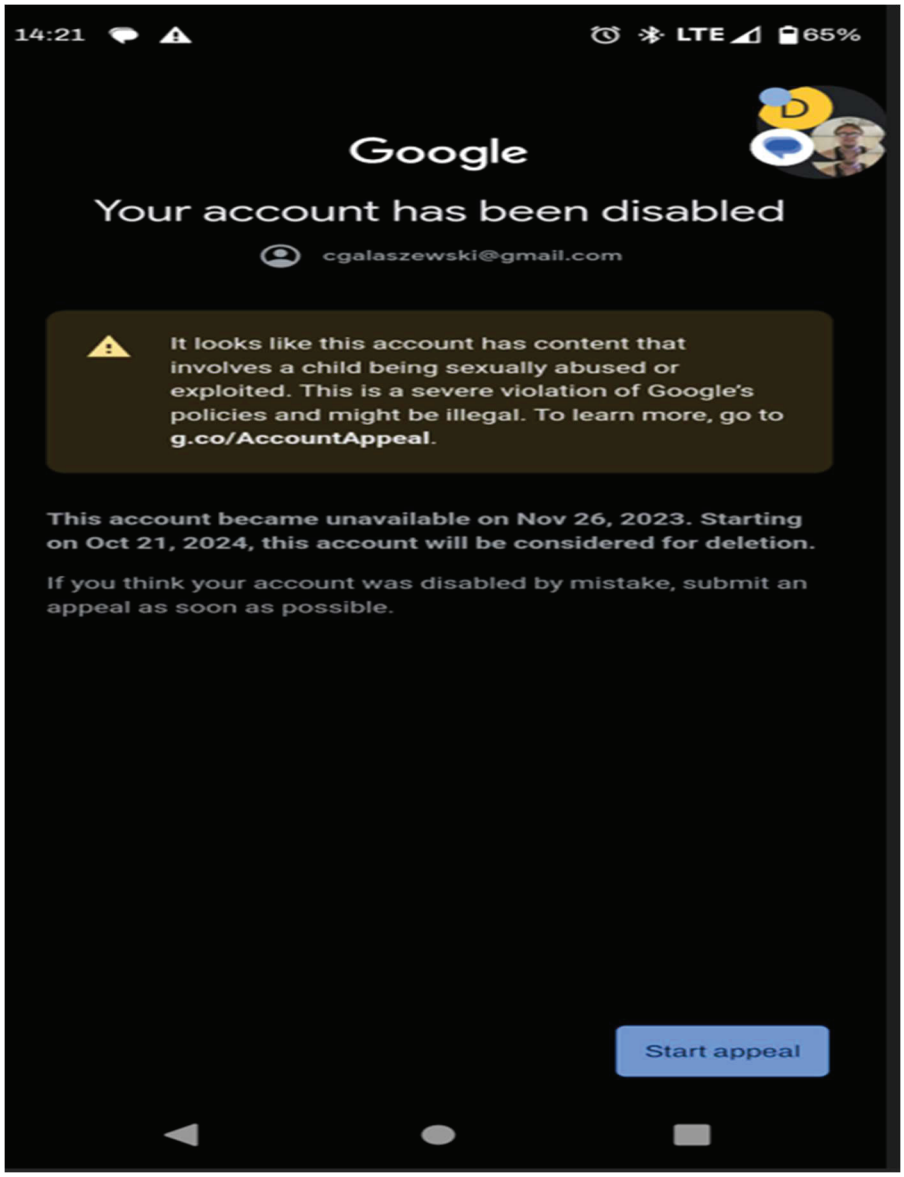
24. In September 2023, your Affiant began investigating Christopher GALASZEWSKI, a registered sex offender, for distributing files depicting suspected child sexual abuse material (CSAM) using an online messaging application that was being monitored by law enforcement. GALASZEWSKI was previously incarcerated by the State of Ohio from 08/07/2018 to 06/09/2023 for convictions related to Rape (Ohio Revised Code 2907.02 5) and Gross Sexual Imposition (Ohio Revised Code 2907.05.5). Your Affiant learned that at the time of this investigation GALASZEWSKI was on active Parole/Supervision with Ohio Adult Parole Authority (APA) Officer Brendan Centeno. Further, your Affiant learned that GALASZEWSKI was arrested by Officer Centeno on November 28, 2023, and subsequently returned to prison for violating terms of his Parole/Supervision (Expected release date is 08/23/2024).

25. Officer Centeno provided a copy of his Violation Report for GALASZEWSKI to your Affiant for review. In this report, Officer Centeno wrote that on November 26, 2023, he received multiple text messages and phone calls from GALASZEWSKI stating that his second phone (216-290-8900) had been hacked. Officer Centeno described GALASZEWSKI as "very nervous", and wrote that GALASZEWSKI stated, "he didn't do anything and that there was child porn on his Gmail account (cgalaszewski@gmail.com) because it was hacked". When Officer Centeno asked what exactly was on the phone, GALASZEWSKI stated, "a couple pictures but that he had deleted them". Officer Centeno instructed GALASZEWSKI not to touch or delete anything on the phone and scheduled a meeting with him (**NOTE:** Your Affiant confirmed with Officer

Centeno that when GALASZEWSKI contacted him on this day, he was residing at the City Mission located at XXXX Carnegie Avenue, Cleveland, Ohio 44103).

26. Officer Centeno's Violation Report indicated that he met GALASZEWSKI at the City Mission in Cleveland on November 28, 2023, and GALASZEWSKI admitted to having over 100 pictures of child pornography on his Android cellphone. Further, GALASZEWSKI showed Officer Centeno where they were located on the device. Officer Centeno reviewed some of these files and confirmed that they depicted what he identified as child pornography. During his arrest of GALASZEWSKI, Officer Centeno seized an iPhone, Android phone, and an HP laptop from him.

27. On February 22, 2024, your Affiant obtained a search warrant from United States Magistrate Judge Thomas M. Parker (Case No. 1:24-mj-3019 TMP) in the United States District Court for the Northern District of Ohio to search the electronic devices that Officer Centeno seized from GALASZEWSKI. While reviewing the electronic contents of a Motorola, Moto G Play, cellphone (IMEI # 359687212362090) pursuant to this warrant your Affiant observed numerous user attributes and activity (to include selfie style pictures) that linked it to GALASZEWSKI. Further, your Affiant observed that the user of this cellphone sent the following image using text message to "C Blue", "Mom", and "Dad":



In conjunction with this image, your Affiant observed a text reading "I am going to prison" was sent to "C Blue" on 11/26/2023 at 7:23:59 PM (UTC +0). The individual pictured in the upper right-hand

corner of this file matches multiple images of GALASZEWSKI that your Affiant has seen. Lastly, while reviewing this device, your Affiant observed multiple files of suspected CSAM including the lascivious exhibition of child's genitals, as well as at least one (1) file depicting a toddler being sexually penetrated by an adult male's erect penis.

28. On March 22, 2024, your Affiant asked Ohio Internet Crimes Against Children (ICAC) Task Force Criminal Analyst (C/A) Caroline Wathey to conduct a check of the ICAC Data System (IDS) for the email address **cgalaszewski@gmail.com**, that was displayed in the image pictured in paragraph 27. IDS is a database that allows law enforcement to see if any number of unique identifiers, to include email addresses, have been previously associated with an ICAC investigation involving CSAM. The IDS database also checks to see if these unique identifiers are associated with any NCMEC Cyber Tipline Reports. This check indicated that this email address was associated with a Cyber Tipline Report that was previously made to NCMEC.

29. On November 27, 2023, the Electronic Service Provider (ESP) Google submitted Cyber Tipline (CT) Report 180609808 to NCMEC regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Name:	Christopher Galasezwski
Phone:	+12164234688 (Verified 11-16-2023) +14409411745 (Verified 07-29-2023) +12162908900 (Verified 09-06-2023)
Date of Birth:	06-16-1998
Email Address:	cgalaszewski@gmail.com (Verified)

mckainchris3@gmail.com

ESP User ID: RGQXX2MYHJVIQ65YG262CHWWUI

Google reported that on November 26, 2023, this user uploaded seventeen (17) files of apparent child pornography over the Google Gmail infrastructure. Google reported these files were uploaded on November 26, 2023, between 18:40:50 hours UTC and 18:41:11 hours UTC from IP address 2607:fb90:b52d:8fad:275b:b87f:4671:a624. Google, after viewing the content of one (1) of these files (Filename "4cc96377f2c701dfbaca51f287f7c889-1969_28_02_17_7_16_44.jpeg"), provided them all to NCMEC as part of their CT Report. The remaining sixteen (16) files of apparent child pornography that Google provided as part of their CT Report that they did not view were identified based on their unique hash values which were previously identified as depicting apparent child pornography. Based on an initial check of the IP address utilized by these accounts when the files of child pornography were uploaded, this activity occurred near Cleveland, Ohio, so this CT was forwarded to the Ohio ICAC Task Force.

30. On March 22, 2024, C/A Wathey provided your Affiant with a copy of the CT Report as well as Filename "4cc96377f2c701dfbaca51f287f7c889-1969_28_02_17_7_16_44.jpeg" for review. As noted in paragraph 29, this was the file that a representative from Google viewed before submitting the CT to NCMEC. (**NOTE:** C/A Wathey did not provide the other sixteen (16) files submitted by Google as part of this CT, and your Affiant has not viewed them.) Your Affiant viewed this file which depicts suspected CSAM and can be more fully described as follows:

a. This image file has two watermarks that read "Lolitas Content" and depict a nude early pubescent female squatting down with her legs spread wide and her hands on her knees. The child's vagina is clearly visible in the image and appears as the focal point of the image. The child's face is visible, and she is looking directly at the camera.

31. Your Affiant observed that the day Google reported these files of suspected CSAM were uploaded to their servers, November 26, 2023, was also the same day that GALASZEWSKI reported to Officer Centeno that child pornography was in his Gmail account (Paragraph 25). Your Affiant confirmed with Officer Centeno that when GALASZEWSKI contacted him on this day, he was residing at the City Mission in Cleveland, Ohio. Further, Officer Centeno confirmed that when he met with GALAZEWSKI and took him into custody two days later, it occurred at the City Mission. Lastly, your Affiant confirmed that GALAZEWSKI does not have a valid driver's license or have a vehicle registered to him.

32. On March 28, 2024, Ohio ICAC Intake Officer (I/A) Nicole Reedy provided your Affiant with an additional Cyber Tipline Report associated with **mckainchris3@gmail.com**. This report indicated that on June 13, 2023, the Electronic Service Provider (ESP) Dropbox submitted CT Report 164084798 to NCMEC regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Email Address: mckainchris3@gmail.com (Verified 06-13-2023 23:56:10 UTC)

Screen/User Name: Chris Mckain

Dropbox reported that on June 12, 2023, this user uploaded three (3) files of apparent child pornography to this Dropbox account. Dropbox, after viewing the content of all these files, provided them to NCMEC as part of their CT Report. The contents of these files depict the lascivious display of multiple minor female's genitals, anuses, and breasts. An initial check of the IP address used to by **mckainchris3@gmail.com** to upload these files resolved to T-Mobile USA in the Cleveland-Akron metro area. Your Affiant knows that the phones utilized by GALASZEWSKI during this investigation were registered to T-Mobile.

33. On March 28, 2024, your Affiant made a preservation of records request to Google for the account contents/records associated with **cgalaszewski@gmail.com** and **mckainchris3@gmail.com**. On that same day Google responded as follows: "Your preservation – Google Reference Number 56334595 – is now complete and we have preserved the records you identified, to the extent that such data exists. For the account data preserved, in accordance with 18 U.S.C.2703(f), Google will retain these records for a period of 90 days, after which they may be subject to deletion. In addition, as detailed in the Google Account Disable message (Paragraph 27), "This account became unavailable on Nov 26, 2023. Starting on Oct 21, 2024, this account will be considered for deletion.".

34. Based on the information above, your Affiant believes GALAZEWSKI was in the Northern District of Ohio at the time he used **cgalaszewski@gmail.com** and **mckainchris3@gmail.com** to possess and/or distribute child pornography.

35. Further, based on the above information, your Affiant has probable cause to believe that the user of the **cgalaszewski@gmail.com** and **mckainchris3@gmail.com** committed the offense of possessing and/or distributing child pornography, in violation of Title 18, United States Code, §§2252A and that information contained within this account and maintained at Google will assist myself and law enforcement in identifying the person or persons using this account. As noted above, the accounts **cgalaszewski@gmail.com** and **mckainchris3@gmail.com** were both reported by Google as being associated with the upload of apparent CSAM. Additionally, an account associated with **mckainchris3@gmail.com** was further reported by Dropbox for uploading apparent CSAM.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. Your Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

37. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of Google there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that the Google email accounts described

in Attachment A will contain evidence of a crime, specifically but not limited to, identification of the person who possessed and/or distributed files of child pornography through the Google accounts discussed above. Accordingly, a search warrant is requested.

38. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Jason M. Guyton
Special Agent
Homeland Security Investigations

Sworn to via telephone after submission by reliable electronic means [Fed. R. Crim. P. 4.1 and 41(d)(3)] on this 4th day of April 2024.

REUBEN J. SHEPERD
UNITED STATES MAGISTRATE JUDGE